(ISC)²®

Chapter 5 Resource

Security Operations

Chapter Summary

This chapter focused on the day-to-day, moment-by-moment, use of security controls and risk mitigation strategies in an organization. We discovered ways to secure data and the systems they reside on. Data (information) security as a process and discipline provides a structure for protecting the value of data as the organization creates, stores, shares, uses, modifies, archives and finally destroys that data (known as data handling). During data handling, an organization classifies (assigns data sensitivity levels), categorizes (determines type of data), labels (applies a name to the data), retains (determines how long to keep the data) and destroys (erases or destroys) the data.

A best practice for securing data is encrypting the data. We explored the process of encrypting data in plaintext with a key and algorithm to create ciphertext then using either the same key (symmetric) or a different key (asymmetric) and same algorithm to decrypt the ciphertext to convert it back to plaintext. Then hashing was methodically described; hashing takes an input set of data (of almost arbitrary size) and returns a fixed-length result called the hash value.

System hardening is the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems and software, including operating system, web server, application server, application, etc. We also discussed configuration management, a process and discipline used to ensure that the only changes made to a system are those that have been authorized and validated. Configuration management consists of identification, baseline, change control, and verification and audit. During configuration management, one must conduct inventory, baselines, updates, and patches.

The following best practice security policies were examined: data handling (appropriate use of data), password (appropriate use of passwords), acceptable use (appropriate use of the assets, devices, and data), bring your own device (appropriate use of personal devices), privacy (appropriate protection of one's privacy), and change management (appropriate transition from current state to a future state). Change management practices address a common set of core activities: documentation, approval, and rollback. It starts with a request for change (RFC) and moves through various development and test stages until the change is released to the end users.

We ended the chapter by discussing the importance of security awareness training and how it reduces the internal threat to an organization. By breaking down the levels of security awareness training into education, training, and awareness, we identified that the training can be tailored to the security topic(s), organization, position and/or individual. We also emphasized the importance of password protection.

Module Names

Module 1: Understand Data Security

Module 2: Understand System Hardening

Module 3: Understand Best Practice Security Policies

Module 4: Understand Security Awareness Training

Chapter to Domain Mapping

Module Number	Module Title	Domains
1	Understand Data Security	5.1, 5.1.1, 5.1.2, 5.1.3
2	Understand System Hardening	5.2, 5.2.1
3	Understand Best Practice Security Policies	5.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.3.6
4	Understand Security Awareness Training	5.4, 5.4.1, 5.4.2, 5.3.2

Learning Objectives

After completing this chapter, the participant will be able to:

- Explain concepts of security operations
- Discuss data handling best practices
- Identify key concepts of logging and monitoring
- Summarize the different types of encryption and their common uses
- Describe the concepts of configuration management
- Explain the application of common security policies
- Discuss the importance of security awareness training
- Practice the terminology of and review the concepts of network operations

Chapter Takeaways

Module 1: Understand data security

Data handling process:

- Create
- Store
- Share
- Use
- Modify
- Archive
- Destroy

Examples of data sensitivity levels:

- Highly restricted: Compromise of data with this sensitivity label could possibly put the organization's future existence at risk. Compromise could lead to substantial loss of life, injury or property damage, and the litigation and claims that would follow.
- Moderately restricted: Compromise of data with this sensitivity label could lead to loss of temporary competitive advantage, loss of revenue, or disruption of planned investments or activities.
- Low sensitivity (sometimes called "internal use only"): Compromise of data with this sensitivity label could cause minor disruptions, delays or impacts.
- Unrestricted public data: As this data is already published, no harm can come from further dissemination or disclosure.

Logging - Ingress monitoring tools:

- Firewalls
- Gateways
- Remote authentication servers
- IDS/IPS tools
- SIEM solutions
- Anti-malware solutions

Logging – Egress monitoring data types:

- Email (content and attachments)
- Copy to portable media
- File Transfer Protocol (FTP)
- Posting to web pages/websites
- Applications/application programming interfaces (APIs)

Two primary types of encryption:

- Symmetric – same key
- Asymmetric – different keys

Module 1: Understand data security (continued)

Five functions of a cryptographic hash:

1. Useful: It is easy to compute the hash value for any given message.
2. Nonreversible: It is computationally infeasible to reverse the hash process or otherwise derive the original plaintext of a message from its hash value (unlike an encryption process, for which there must be a corresponding decryption process).
3. Content integrity assurance: It is computationally infeasible to modify a message such that re-applying the hash function will produce the original hash value.
4. Unique: It is computationally infeasible to find two or more different, sensible messages that hash to the same value.
5. Deterministic: The same input will always generate the same hash, when using the same hashing algorithm.

Module 2: Understand system hardening

Configuration management procedures:

- Identification
- Baseline
- Change control
- Verification & Audit

Elements of configuration management:

- Inventory
- Baselines
- Updates
- Patches

Module 3: Understand best practice security policies

Best practice security policies:

- Data handling - appropriate use of data
- Password - appropriate use of passwords
- Acceptable use - appropriate use of the assets, devices, and data
- Bring your own device - appropriate use of personal devices
- Privacy - appropriate protection of one's privacy
- Change management - appropriate transition from current state to a future state

Data handling policy procedures:

- Classify
- Categorize
- Label
- Store
- Encrypt
- Backup
- Destroy

Module 3: Understand best practice security policies (continued)

Examples: Password policy procedures

- Password creation:
  - All user and admin passwords must be at least a certain length. Longer passphrases are encouraged.
  - Passwords cannot be the same or similar to other passwords used on any other websites, system, application or personal account.
  - Passwords should not be a single word or a commonly used phrase.
  - Avoid passwords that are easy to guess, such as the names and birthdays of your friends and family, your favorite bands or catchphrases you like to use.
  - Dictionary words and phrases should be avoided.
  - Default installation passwords must be changed immediately after installation is complete.
- Password aging:
  - User passwords must be changed on a schedule established by the organization. Previously used passwords may not be reused.
  - System-level passwords must be changed according to a schedule established by the organization.
- Password protection:
  - Passwords must not be shared with anyone, even IT staff or supervisors, and must not be revealed or sent electronically. Do not write down your passwords.

Acceptable use policy (AUP) procedures:

- Data access
- System access
- Data disclosure
- Passwords
- Data retention
- Internet usage
- Company device usage

Possible devices on the bring your own device (BYOD) policy:

- Cell phone
- Tablet
- Laptop
- Smartwatch
- Bluetooth devices

Privacy policy protects:

- PII
- ePHI
- Bank/credit card information

Examples of national and international privacy regulations/laws:

- GDPR in the EU
- Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada

Module 3: Understand best practice security policies (continued)

Change management policy consists of three major activities:

- Deciding to change
- Making the change
- Confirming that the change has been correctly accomplished

Module 4: Understand security awareness training

Security awareness training types:

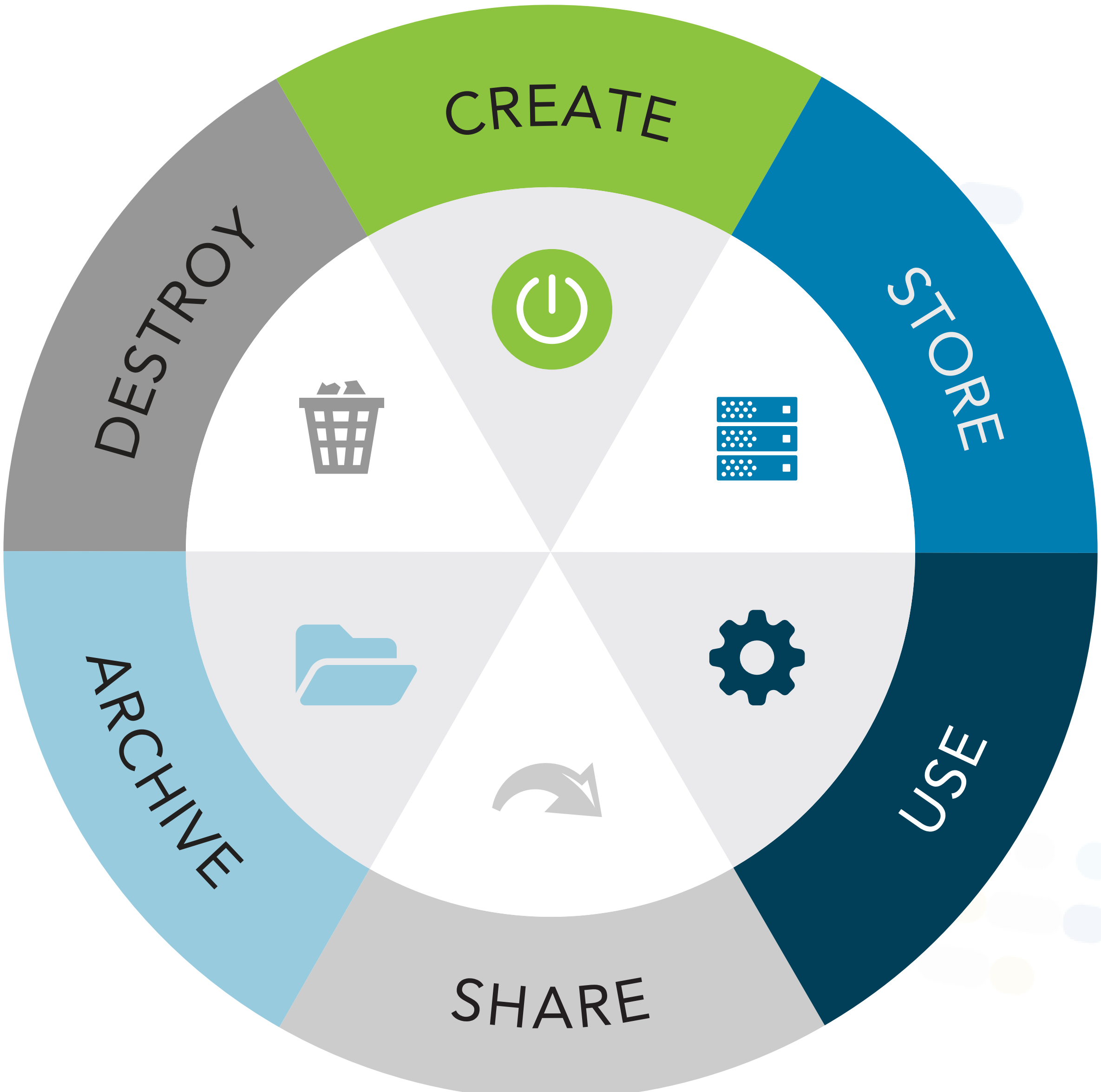
- Education
- Training
- Awareness

Some social engineering techniques:

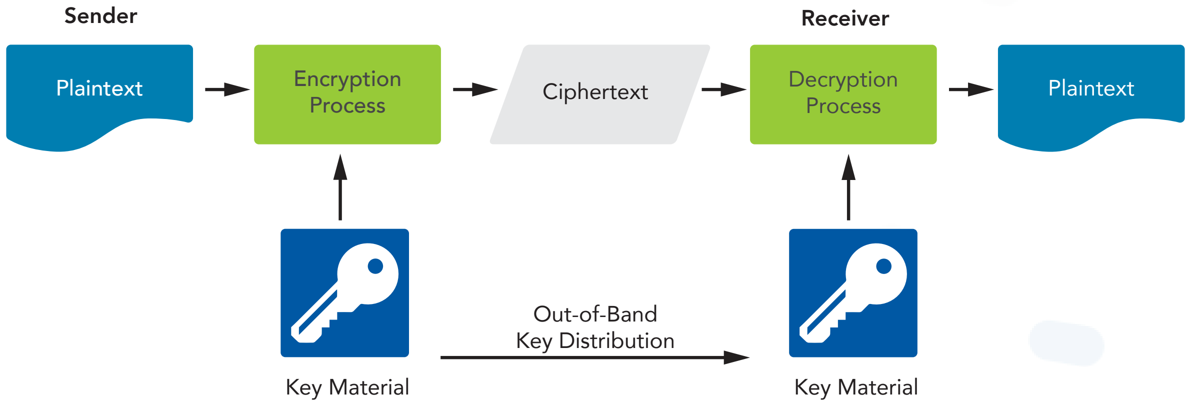
- Baiting
- Phone phishing or vishing
- Pretexting
- Quid pro quo
- Tailgating
- False flag or false front operations

Graphics

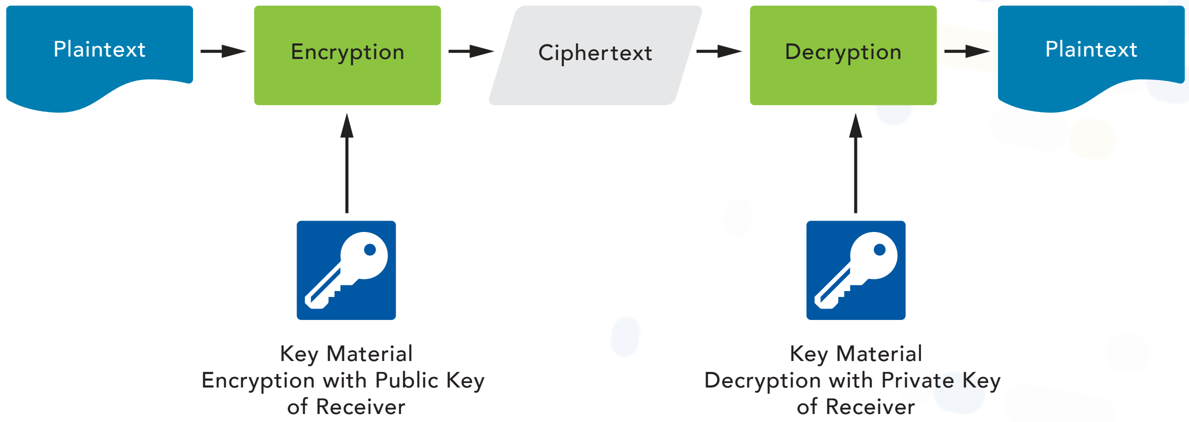
Data Security Lifecyle



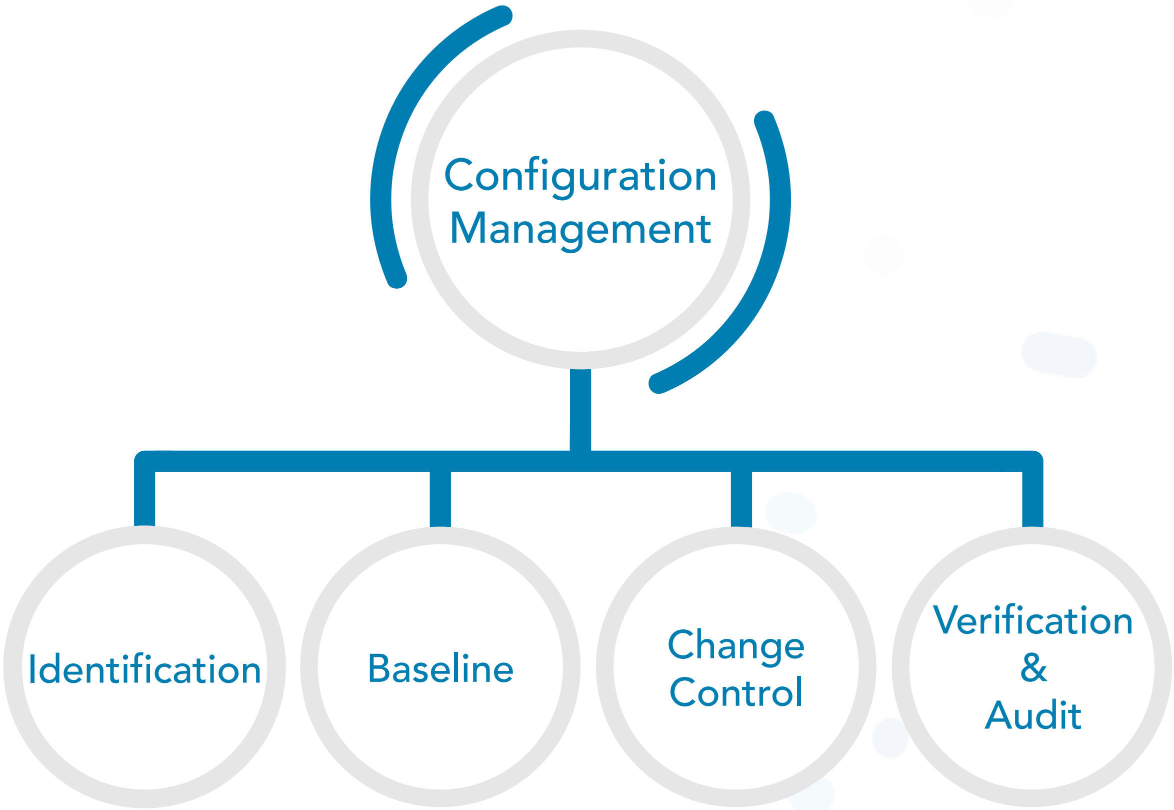
Use of Symmetric Algorithms



Use of Asymmetric Cryptography to Send a Confidential Message

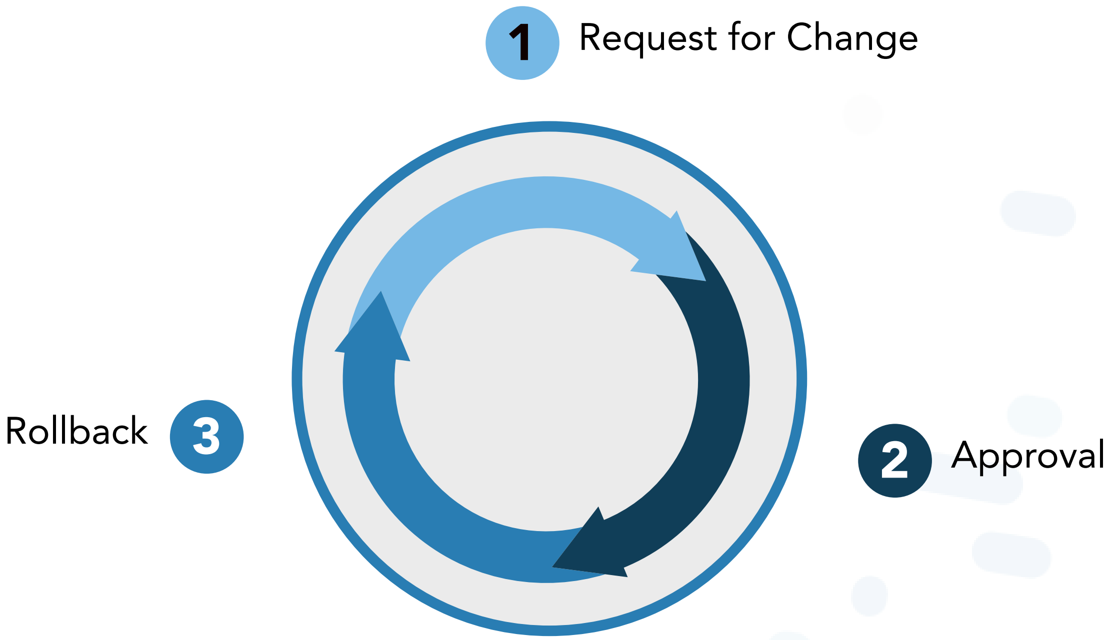


Configuration Management



Change Management Components

Change Management Components



Formulas and Calculations

Cryptographic Hash Function

variable data input

+

hashing algorithm

=

fixed bit size data output (the digest)

Chapter Terms and Definitions

Application Server

A computer responsible for hosting applications to user workstations. NIST SP 800-82 Rev.2

Asymmetric Encryption

An algorithm that uses one key to encrypt and a different key to decrypt the input plaintext.

Checksum

A digit representing the sum of the correct digits in a piece of stored or transmitted digital data, against which later comparisons can be made to detect errors in the data.

Ciphertext

The altered form of a plaintext message so it is unreadable for anyone except the intended recipients. In other words, it has been turned into a secret.

Classification

Classification identifies the degree of harm to the organization, its stakeholders or others that might result if an information asset is divulged to an unauthorized person, process or organization. In short, classification is focused first and foremost on maintaining the confidentiality of the data, based on the data sensitivity.

Configuration management

A process and discipline used to ensure that the only changes made to a system are those that have been authorized and validated

Cryptanalyst

One who performs cryptanalysis which is the study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.

Cryptography

The study or applications of methods to secure or protect the meaning and content of messages, files, or other information, usually by disguise, obscuration, or other transformations of that content and meaning.

Data Loss Prevention (DLP)

System capabilities designed to detect and prevent the unauthorized use and transmission of information.

Decryption

The reverse process from encryption. It is the process of converting a ciphertext message back into plaintext through the use of the cryptographic algorithm and the appropriate key for decryption (which is the same for symmetric encryption, but different for asymmetric encryption). This term is also used interchangeably with the "deciphering."

Degaussing

A technique of erasing data on disk or tape (including video tapes) that, when performed properly, ensures that there is insufficient magnetic remanence to reconstruct data.

Digital Signature

The result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation. NIST SP 800-12 Rev. 1

Egress Monitoring

Monitoring of outgoing network traffic.

Encryption

The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

Encryption System

The total set of algorithms, processes, hardware, software, and procedures that taken together provide an encryption and decryption capability.

Hardening

A reference to the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems, and software, including operating system, web server, application server, application, etc. Hardening is normally performed based on industry guidelines and benchmarks, such as those provided by the Center for Internet Security (CIS).

Hash Function

An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message. NIST SP 800-152

Hashing

The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. Source CNSSI 4009-2015

Ingress Monitoring

Monitoring of incoming network traffic.

Message Digest

A digital signature that uniquely identifies data and has the property such that changing a single bit in the data will cause a completely different message digest to be generated. NISTIR-8011 Vol.3

Operating System

The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations. NIST SP 800-44 Version 2

Patch

A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component. Source: ISO/IEC 19770-2

Patch Management

The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. Source: CNSSI 4009

Plaintext

A message or data in its natural format and in readable form; extremely vulnerable from a confidentiality perspective.

Records

The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items). NIST SP 800-53 Rev. 4

Records Retention

A practice based on the records life cycle, according to which records are retained as long as necessary, and then are destroyed after the appropriate time interval has elapsed.

Remanence

Residual information remaining on storage media after clearing. NIST SP 800-88 Rev. 1

Request for change (RFC)

The first stage of change management, wherein a change in procedure or product is sought by a stakeholder.

Security Governance

The entirety of the policies, roles, and processes the organization uses to make security decisions in an organization.

Social engineering

Tactics to infiltrate systems via email, phone, text, or social media, often impersonating a person or agency in authority or offering a gift. A low-tech method would be simply following someone into a secure building.

Symmetric encryption

An algorithm that uses the same key in both the encryption and the decryption processes.

Web Server

A computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, and Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an "intranet server." NIST SP 800-44 Version 2

Whaling Attack

Phishing attacks that attempt to trick highly placed officials or private individuals with sizable assets into authorizing large fund wire transfers to previously unknown entities.